Advanced Reactor Safeguards & Security

Small Modular Reactor and Microreactor Security-by-Design Lessons Learned: Integrated PPS Designs

Prepared for

U.S. Department of Energy

Alan Evans

Sandia National Laboratories

September 2024

SAND2024-11539R

Prepared by Sandia National Laboratories, Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

ABSTRACT

U.S. nuclear power facilities face increasing challenges in meeting dynamic security requirements caused by evolving and expanding threats while keeping costs reasonable to make nuclear energy competitive. The past approach has often included implementing security features after a facility has been designed and without attention to optimization, which can lead to cost overruns. Incorporating security into the design process can provide robust, cost-effective, and sufficient physical protection systems. The purpose of this report is to capture lessons learned by the Advanced Reactor Safeguards and Security (ARSS) program that may be beneficial for other advanced and small modular reactor (SMR) vendors to use when developing security systems and postures. This report will capture relevant information that can be used in the security-by-design (SeBD) process for SMR and microreactor vendors.

ACKNOWLEDGEMENTS

We would like to acknowledge the DOE Office of Nuclear Energy Advanced Reactor Safeguards and Security (ARSS) program for funding this crucial work to partner with U.S. domestic SMR and microreactor vendors. We would also like to thank the many subject matter experts from Sandia National Laboratories, including Doug Abell, Jason Davenport, Emily Sandt, David Lee, Ben Stromberg, Ian Steagall, and Matt Erdman, for contributing to this work.

CONTENTS

1. General Lessons Learned for Small Modular Reactors 8
   1.1. Security-by-Design 8
   1.2. Deployment Locations and Impacts on Physical Protection Systems 9
   1.3. Unique Sabotage Considerations 10
   1.4. Protecting Plant Capital and Industrial Systems 11
2. Intrusion Detection System Design 13
   2.1. Design Basis Threat Considerations for Intrusion Detection Systems 13
   2.2. Performance Measures for an Intrusion Detection System 14
   2.3. Sensor Design 15
      2.3.1. External Intrusion Detection Systems/Perimeter Intrusion Detection and Assessment Systems 16
         2.3.1.1. Advanced Perimeter Intrusion Detection Sensors 18
   2.4. Assessment Designs 19
   2.5. Central Alarm Station and Backup Alarm Stations 21
3. Integrated Physical Protection System Design 23
   3.1. Building Design and Response Force Strategy 24
   3.2. Staffing Plans 26
      3.2.1. Total System Failure 27
      3.2.2. Personnel Access 27
      3.2.3. Vehicle and Material Access and Escort 27
4. Conclusions 29

LIST OF FIGURES

Figure 1. Security-by-Design Based on DEPO Methodology 8
Figure 2. Remote Microreactor Deployment 10
Figure 3. Pressurized Water Reactor Safety Functions and Front Line Systems[3] 11
Figure 4. Alarm Initiation and Assessment Process 13
Figure 5. Conditions that Affect Exterior Sensors 15
Figure 6. PIDAS Example 16
Figure 7. PIDAS Sensor Configuration Example 17
Figure 8. Defense-in-Depth Intrusion Detection System Design 18
Figure 9. Exterior Sensors (Left: Dual Stack Bistatic Microwave Sensors. Right: Active Infrared Sensors) 18
Figure 10. Monitor View of an Assessment Zone 20
Figure 11. Levels of Resolution for Video Assessment Systems 20
Figure 12. Alarm Communication & Display System 21
Figure 13. Adversary Task Time Compared to PPS Response Time 24
Figure 14. Square Building Design 25

LIST OF TABLES

Table 1. Required NRC Security Positions under 10 CFR 73.55 26
Table 2. Accounting for Anomalies Meeting NRC Regulations in 10 CFR 73.55 27
Table 3. Alternative Security Staffing Headcount 28

This page left blank

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
AC&D	alarm communication and display
ARSS	Advanced Reactor Safeguards and Security (program)
ASO	armed security officer
BAS	backup alarm station
BBRE	bullet- and blast-resistant enclosure
CAS	central alarm station
CFR	Code of Federal Regulations
CCTV	closed circuit television
CPD	critical detection point
DBT	design basis threat
DEPO	design and evaluation process outline
DMA	deliberate motion analytics
ECP	entry control point
FAR	false alarm rate
FTE	full-time equivalent
IDS	intrusion detection system
INS	see Section 1 – include?
LLEA	local law enforcement agency
NAR	nuisance alarm rate
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
Pa	probability of assessment
PA	protected area
Pd	probability of detection
PIDAS	perimeter intrusion detection and assessment system
PIDS	perimeter intrusion detection system
PPS	physical protection system
Ps	probability of sensing
PWR	pressurized water reactor
RTL	response team lead
SeBD	security-by-design
SMR	small modular reactor
Ta	assessment and communication time
VBED	vehicle-borne explosive device

1. GENERAL LESSONS LEARNED FOR SMALL MODULAR REACTORS

Throughout Sandia National Laboratories' engagements funded by the DOE's Office of Nuclear Energy Advanced Reactor Safeguards and Security (ARSS) program with U.S. small modular reactor (SMR) and microreactor vendors, many lessons have been learned in regard to designing and evaluating a physical protection system (PPS). This report captures those lessons learned to help inform better system and security design in the future.

1.1. Security-by-Design

Lesson Learned: SMR and microreactor vendors should ensure that all necessary stakeholders are integrated into the security-by-design (SeBD) process.

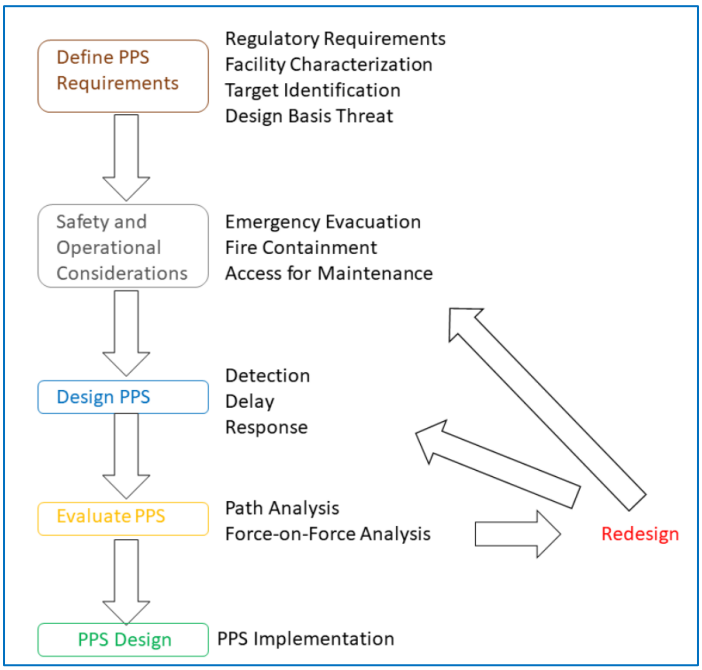

Figure 1. Security-by-Design Based on DEPO Methodology[1]

U.S. SMR and microreactor vendors should ensure that all relevant stakeholders who may be impacted are involved in decisions and discussions about any necessary changes needed to ensure an effective PPS. During our engagements with multiple SMR and microreactor vendors, the vendor security teams were being pushed to make design decisions or make changes to the PPS design based on needed changes for safety system designs and operation designs. While these decisions are necessary to ensure safe operations of any nuclear facility, it is recommended that the security team for the vendor be involved in the decision-making process and overall planning process for these changes to the facility. First, this allows the security design team to understand why the change needs to be made and allows for the vendor security team to propose an adequate design change for

[1] "U.S. Domestic Pebble Bed Reactor: Security-by-Design." A. Evans, S. Horowitz, C. Evans, B. Stromberg, R. Knudsen. Sandia National Laboratories. SAND2021-13122 R.

the security system. Second, this allows all stakeholders to understand how small impacts or changes in one area of the plant design might have impacts to other areas of the plant design.

Ensuring that all relevant stakeholders are involved in decision-making that affects the plant layout will reduce the burden on each individual stakeholder in the long run. For example, if a building needs to be added to the facility layout to support plant operations, this building may have significant impacts on the PPS design and involve major changes for the security team. When a new building or structure gets added to the site, the PPS team may have to reanalyze adversary pathways, evaluate if the current response force strategy is still effective and if the strategy is not still effective, the PPS team may have to make changes to the strategy. This additional building may result in the need for another responder in the PPS strategy and may result in less cost-savings due to this additional responder. However, if the operations team discussed this need and change with the PPS team, the two groups could work together to identify a solution that may not impact the overall PPS design and allow for a cost-effective solution to be developed.

1.2. Deployment Locations and Impacts on Physical Protection Systems

Lesson Learned: Evaluate potential deployment locations for unique characteristics that may impact the PPS design and technologies being chosen.

Many SMR and microreactor vendors are considering deployment in multiple locations with various environmental and weather conditions that may impact the design of the PPS and the technologies chosen to be implemented in a PPS. For example, vendors pursuing deployment options in Texas and Alaska will face different environmental and weather conditions. A deployment in Texas could consider traditional PPS technologies that have been used at nuclear deployments in Texas. Deployment in Alaska may require the vendor to determine things such as annual snowfall, annual rainfall, the maximum amount of snowfall over a 24-hour period, and many other considerations. Weather in the deployment location may require the vendor or the operator of an SMR or microreactor to choose specific PPS technologies that are most effective in the deployment location. Additional considerations should be taken when designing a vehicle barrier system and other delay measures at the facility. For example, siting locations where the depth of digging is limited may impact the type of vehicle barriers can be used at the facility. These environmental factors may also determine if power and communication lines can be trenched under the ground or if they need to be routed above-ground. These factors will impact the overall design of the PPS.

Additionally, the deployment location and the environment in that location may have large impacts on the overall PPS design and PPS strategy that can be implemented. When considering the deployment locations, consideration should be made for the personnel working at the facility. For example, if the facility is deployed in a remote location far from where plant personnel may live, there may be delays in getting replacements onsite or long response times for an offsite response force or for a local law enforcement agency (LLEA) to provide additional response. Longer response times required for an offsite response force may require the facility design to have more delay barriers and therefore increase the cost of the initial PPS design and overall facility build. A longer response time for LLEA may require the facility to consider additional methods to increase delay time or hold an adversary force using contingency plans to allow for the additional LLEA officers to arrive to the facility. PPS designers should also consider how the adversaries may be able to use the long distance to their advantage if an offsite response force is used or for additional LLEA response. Adversaries could create roadblocks, cause accidents on the road, or other create scenarios that may increase the overall travel time to the site.

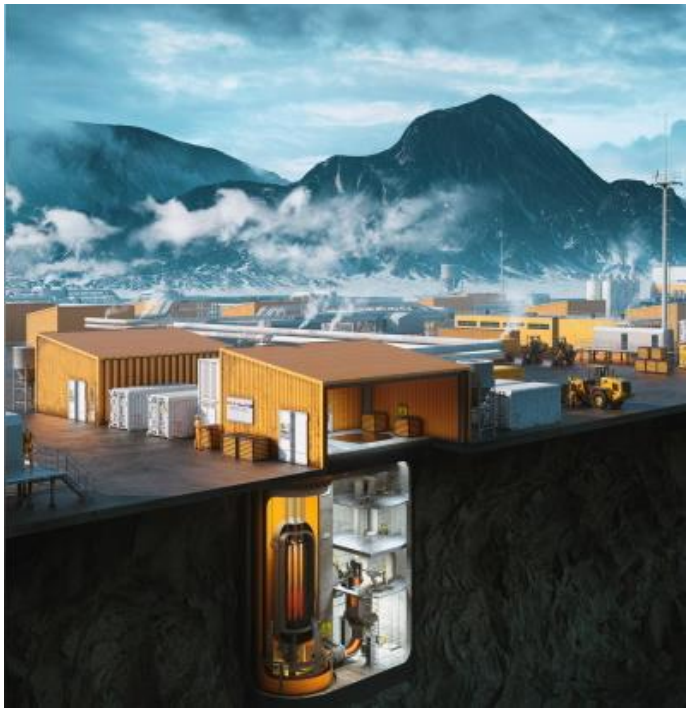

Figure 2. Remote Microreactor Deployment[2]

1.3. Unique Sabotage Considerations

> **Lesson Learned**: SMR and microreactor vendors with novel designs should evaluate unique sabotage considerations and material theft scenarios that are specific to their design.

SMR and microreactor vendors and future operators should consider any potential unique sabotage scenarios that may apply to their reactor design. Similar to various types of large light water reactors having different sabotage scenarios that could result in a radiological release (i.e., U.S. pressurized water reactors [PWR] and Russian VVER reactors), SMRs and microreactors have different sabotage scenarios based on their overall design. For example, it is known that sodium and water may have violent explosions and consequences; this may require SMR designers to evaluate how these interactions could occur and then identify mitigation measures that could prevent these interactions from happening.

These unique sabotage scenarios may be identified through the traditional vital area identification method[3]. The figure below shows the primary safety functions for a PWR. These same safety functions exist for SMRs and microreactors as well. However, the front-line systems may be different. Due to the unique interactions that may result in radiological release, SMR and microreactor vendors should identify if these interactions can occur in their design. SMR and microreactor vendors should also conduct "red teaming," where the vendor determines how an adversary team may cause these interactions to occur and achieve a sabotage event that could cause a radiological release. These red teaming activities allow the vendor and the PPS teams to identify how

[2] https://www.world-energy.org/article/34817.html

[3] "Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants." B Varnado, D. Whitehead. Sandia National Laboratories. September 2008.

these interactions could occur and identify solutions and PPS measures that could mitigate from these events occurring.

Safety Function	Front Line System
Control reactivity	(a) Reactor protection system (b) High pressure injection system
Remove core decay heat and stored heat	(a) Power conversion system (b) Emergency feedwater system (c) High pressure injection system and pressurizer relief valves (feed and bleed) (d) Low pressure injection system (e) Residual heat removal system
Maintain integrity of primary reactor coolant boundary (pressure control)	Pressurizer safety relief valves
Maintain primary coolant inventory	(a) High pressure injection system (b) Low pressure injection system
Protect containment integrity (isolation, overpressure)	(a) Containment spray system (b) Containment cooling system
Scrub radioactive materials from containment atmosphere	(a) Containment spray system (b) Containment ventilation system
Remove irradiated fuel decay heat	Spent fuel pool cooling system
Maintain integrity of irradiated fuel storage	Spent fuel pool
Maintain integrity of radioactive waste storage	(a) Gaseous waste processing system (b) Liquid waste processing system (c) Solid waste processing system

Figure 3. Pressurized Water Reactor Safety Functions and Front Line Systems[3]

1.4. Protecting Plant Capital and Industrial Systems

Lesson Learned: Protecting plant capital and industrial systems should be considered within the design process and be offered some protection by the PPS.

Through our engagements with many industry partners, plant capital and industrial systems have been identified by some SMR and microreactor vendors as important for the continual operation of the facility. This equipment is costly . Plant capital or industrial systems may include systems needed for energy conversion (i.e., turbines, generators, switchyards, energy storage) or equipment necessary for industrial applications (i.e., energy storage, overhead cranes, refueling buildings and equipment). If sabotaged, these systems and equipment may not lead to a radiological release, but they may disrupt plant operations and cost the vendor or the operator large amounts of money to replace, as well as potential loss of revenue. One recommendation to protect plant capital equipment or industrial systems is to place them at least within the protected area (PA) of the facility. This would afford protection of these items through the intrusion detection system (IDS), vehicle barriers, additional delay measures, and a response force if an onsite response force is used. This may lead to

a slight increase in the initial PPS costs by having a larger PA and vehicle barrier perimeter but may reduce the risk and costs if these items are lost due to sabotage by an adversary.

2. INTRUSION DETECTION SYSTEM DESIGN

PPSs consist of three primary functions: detection, delay, and response. Detection, especially at the perimeter of a facility, plays a crucial role in developing an effective PPS.

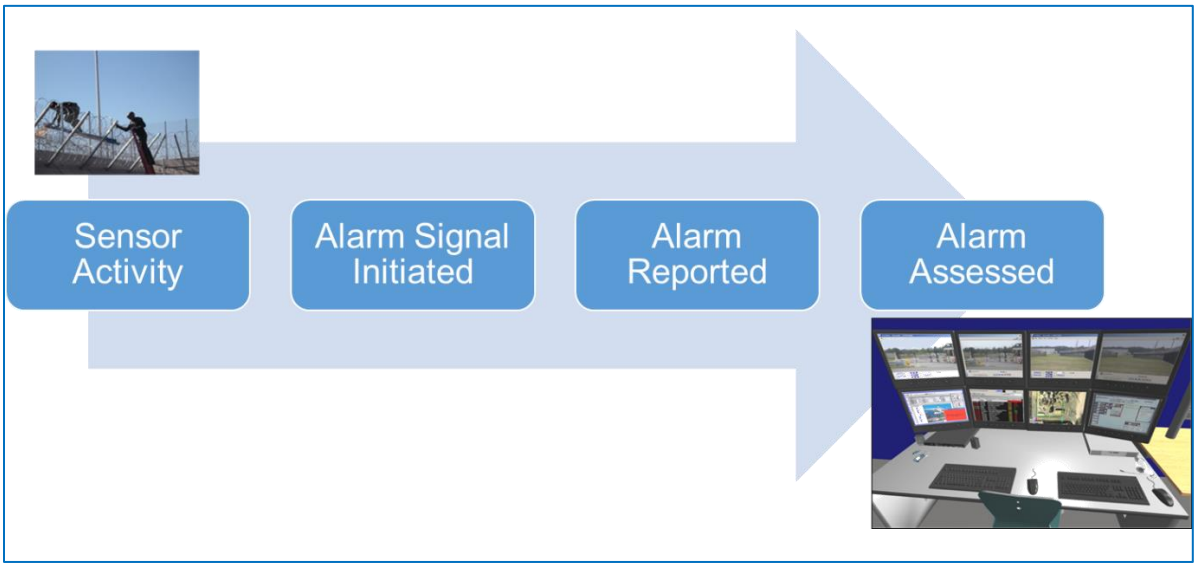

Figure 4. Alarm Initiation and Assessment Process[4]

2.1. Design Basis Threat Considerations for Intrusion Detection Systems

Lesson Learned: The design basis threat (DBT) is an important factor that impacts the design of an IDS, and vendors must ensure their IDS design is capable of detecting an adversary incursion into the facility.

The DBT provided by the U.S. Nuclear Regulatory Commission (NRC) will provide vendors and operators with the information a PPS should be designed to protect against. This DBT will identify to the vendors and operators how many adversaries they must protect against, the tools that the adversary team can use in an adversary attack, the knowledge, skills, and abilities of the adversary, and will define how an adversary team may choose to attack the facility.

Vendors should use the information in the DBT to effectively design their IDS. Vendors should consider the number of adversaries that may attack the facility and that adversaries may choose to attack the facility in multiple groups. If the adversary can attack the facility in multiple groups, then the IDS should be designed by the vendor to ensure that the system is capable of detecting and assessing multiple adversary teams attacking the facility at the same time. By using the DBT, vendors can also identify how the tools and capabilities that the adversary will have can defeat or bypass the IDS and avoid detection. Additionally, vendors should note if the DBT has an insider threat. If an insider threat is present in the DBT, the vendor must consider designing things such as tampers and locks into any access point that provides power and communication from any portions of the IDS to the central alarm station (CAS).

[4] "Advanced PIDAS Design Workshop." Sandia National Laboratories, SAND2024-05626PE.

2.2. Performance Measures for an Intrusion Detection System

Lesson Learned: SMR and microreactor vendors should consider the performance measures that are necessary to design an effective IDS. By understanding these performance measures, vendors can identify the most cost-effective solutions for their IDS design.

IDSs can be characterized by the following performance characteristics:

- Probability of sensing (Ps): The probability that a sensor technology can identify a change to the environment and initiate an alarm.
- Probability of assessment (Pa): The probability that a CAS operator can properly identify the cause of an alarm through the use of cameras and other methods of assessment.
- Assessment and communication time (Ta): The time it takes for a CAS operator to assess the alarm cause and communicate this alarm cause to a response force.
- Nuisance alarm rate (NAR): The rate at which the IDS receives alarms that are not caused by an adversary but can be attributable to another source (e.g., animals, weather, faulty sensors, etc.).
- False alarm rate (FAR): The rate at which the IDS receives alarms that cannot be attributed to a source.
- Probability of detection (Pd): The probability that a technology senses disturbance and that the CAS operator can determine correctly the cause of the alarm.

  Probability of detection can be calculated using the equation below:

$$P_d = P_s x P_a$$

From the above equation, it can be seen that the probability of detection is dependent both upon the probability of sensing and the probability of assessment. Therefore, the IDS should be designed to sense adversary incursions and ensure that the CAS operator can adequately assess and communicate the cause of alarms.

SMR vendors and microreactors should ensure they design their IDS to be effective to sense adversary intrusions and allow for the CAS operator to adequately assess these alarms. As mentioned previously, different factors may impact how vendors design the IDS, including weather, the environment, and the DBT.

Figure 5. Conditions that Affect Exterior Sensors

2.3. Sensor Design

> **Lesson Learned**: SMR and microreactor vendors are very concerned about the overall cost of the PPS design, as well as the cost of maintenance and operations. Vendors should understand the methodologies used to choose effective sensors to design an effective IDS and consider the costs of the technology, operation, and maintenance for the sensors selected.

When vendors are considering what sensors should be included in their IDS, there are many factors that should be taken into consideration, including:

- Requirements for the IDS: Are there performance requirements for the IDS, including a specified probability of detection, nuisance alarm rate, false alarm rate, specific types of sensors (i.e., volumetric sensors, line of detection sensor)?
- Constraints: Do constraints such as terrain, soil conditions, weather, traffic, frequency restrictions, approved lists, or other things exist that may limit which type of sensors can be used?
- Features: Are there specific features such as reliability, costs of technologies, sustainability, compatibility, or vendor support availability required for the design of the IDS?

The factors mentioned above should be identified by the vendors before the any IDS design begins. Following this sensor selection process will allow the vendors to determine which sensor types can be used in the IDS design. Once the sensors for the IDS design have been selected, the vendors can begin designing their IDS.

2.3.1. External Intrusion Detection Systems/Perimeter Intrusion Detection and Assessment Systems

Lessons Learned: SMR and microreactor vendors must consider how their perimeter intrusion detection and assessment system (PIDAS) integrates with the PPS and facilitates an effective response to mitigate adversaries.

In engagements with SMR and microreactor vendors, it has been identified that external IDSs or perimeter intrusion detection and assessment systems (PIDAS) are often overlooked parts of the overall PPS design. However, the PIDAS of a facility may be one of the more costly subsystems of a PPS and it requires a lot of thought and integration.

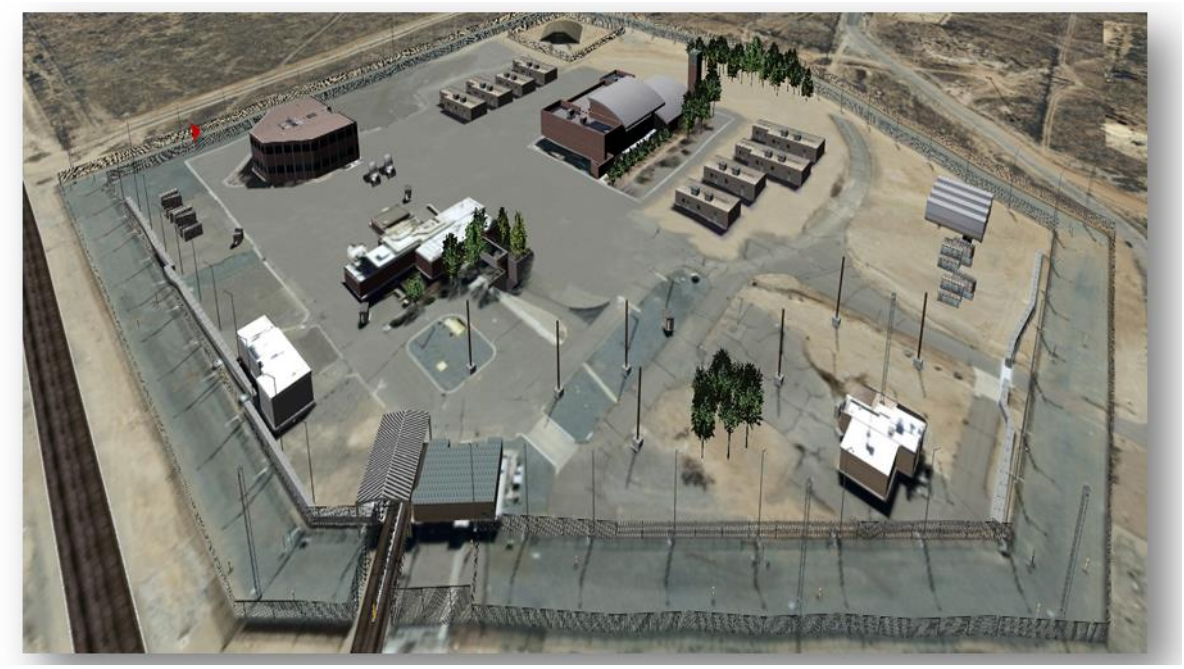

Figure 6. PIDAS Example

When designing a PPS, there are three design principles considered: defense-in-depth, balanced protection, and reliability. These design principles should be applied to all subsystems within the PPS, including a PIDAS. When considering defense-in-depth for a PIDAS, vendors should consider multiple lines of detection to ensure high probabilities of detection and to ensure that adversaries must defeat multiple sensor types to avoid detection at the perimeter of a facility. This ensures that the PPS response timeline can be as long as possible and allow for an effective response to an adversary incursion into the facility. The principle of balanced protection ensures that all portions of the perimeter of the facility, to include entry control points (ECPs), are afforded the same probability of detection around the entire perimeter of the facility. This ensures that there are no adversary pathways into the facility that allow the adversaries to more easily avoid detection than other locations around the perimeter of the facility. The design principle of high reliability should ensure that the sensors selected around the perimeter of the facility have low failure rates and that some redundancy is built into the system to ensure detection at the perimeter of the facility.

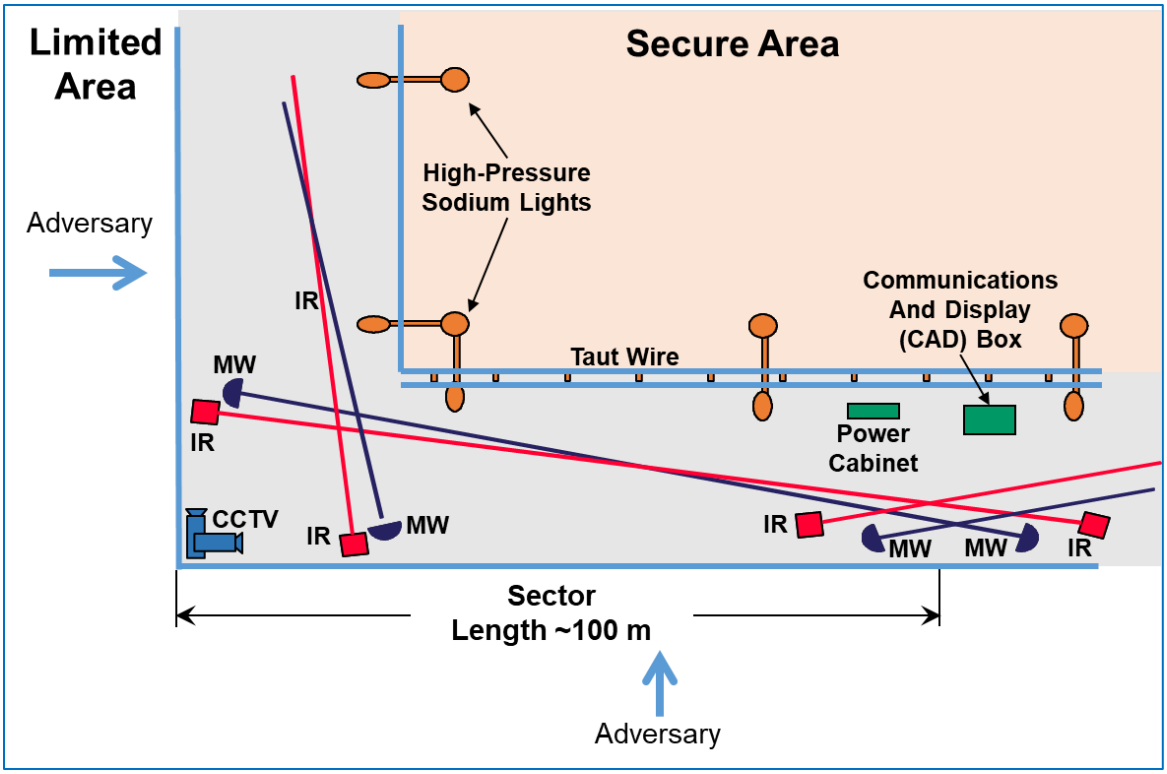

Figure 7. PIDAS Sensor Configuration Example

An additional consideration for vendors is to design their field distribution boxes, which include power and communications to the alarm communication and display (AC&D) system, be placed within the fields of detection provided by the sensors in the PIDAS.

SMR and microreactor vendors should ensure that two lines of detection, using two different sensors, are implemented around the perimeter of the facility. Utilizing two different sensors can help reduce the likelihood that an adversary team could defeat the IDS and avoid detection at the perimeter of the facility. Each sensor has vulnerabilities that can be defeated by bypassing or spoofing the sensor. Bypassing the sensor involves the adversary avoiding the volume of the sensor, or the sensor physics, by crawling, jumping, tunneling, or bridging. Spoofing involves the adversary tricking the sensor into not reporting an alarm. By using at least two different sensors, the PPS can be designed to increase the complexity and/or require multiple defeat types at the perimeter, therefore increasing the probability of detecting an adversary at the perimeter of the facility. The figure below shows how different types of sensors can be used from the perimeter to the target. In the PIDAS, it is best to use a volume sensor (e.g., microwave sensors) and a line detection sensor (e.g., active infrared sensor) if two sensors are to be used. These sensors complement each other in that they have different defeat methods and when designed and installed properly, they can help increase the probability of detection.

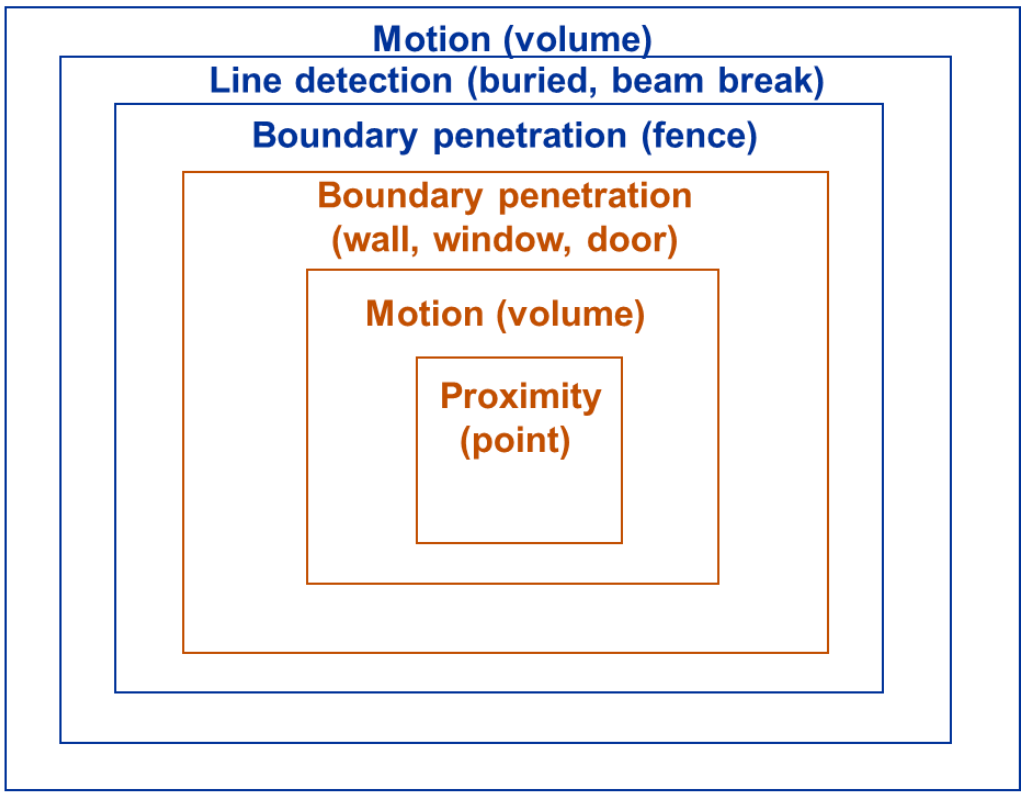

Figure 8. Defense-in-Depth Intrusion Detection System Design

Figure 9. Exterior Sensors (Left: Dual Stack Bistatic Microwave Sensors. Right: Active Infrared Sensors)

2.3.1.1. Advanced Perimeter Intrusion Detection Sensors

Advanced IDS technologies may be available in the near future for some SMR deployments. One example of this technology is deliberate motion analytics (DMA). DMA is a multiple intelligence fusion algorithm for intrusion detection and tracking using a distributed, multi-layer tracking and classification algorithm. DMA's motion pattern recognition algorithms have demonstrated the ability to identify potential intruders inside and outside of the perimeter intrusion detection system (PIDS), issuing alarms against tracks with the correct motion features while filtering out background noise and non-threatening tracks from weather, foliage, and traffic.

Effective utilization of DMA enables individual sensor settings to be set at very sensitive detection thresholds, increasing the probability of sensing a stealthy intruder. Because individual sensors can

be set to a high detection sensitivity, the individual sensors will generate numerous nuisance alarms. However, fusing complementary sensors allows for the potential to eliminate nuisance alarms. Test results to date have shown that the DMA algorithm is capable of effectively filtering out hundreds of thousands of nuisance alarms per day from individual sensors, yielding no nuisance alarms over a period of 1–7 days. DMA has successfully demonstrated the fusion of complementary sensors, including:

1. Radar and video analytics
2. Radar and thermal radar
3. Video analytics and a buried line sensor[5]

While DMA shows promising results for decreasing nuisance alarms as well as upfront capital costs and long-term operation and maintenance costs, DMA has many regulatory hurdles that must be addressed by SMR vendors during the NRC licensing process. Furthermore, the increased timelines provided by earlier detection and assessment are relatively minor compared with the timelines required to implement an effective offsite response strategy. Therefore, significant enhancements in delay features will need to be implemented.

2.4. Assessment Designs

Lesson Learned: Similar to sensor designs, vendors should ensure that effective assessment capabilities exist through well-selected and well-installed camera technologies. Ensuring that adequate cameras are designed into the IDS is an important aspect for designing and implementing an effective PPS to defend against the DBT.

SMR vendors should design an assessment system that integrates with the IDS. The assessment system design should ensure that alarm causes at the perimeter of the facility can be adequately assessed and therefore communicated to the response force to facilitate an effective response. Vendors should ensure that their assessment design, if using closed-circuit television cameras (CCTVs), ensures that each sector is covered by a specific camera. Vendors should also ensure that there is camera overlap around the perimeter of the facility. To achieve this, vendors should ensure that the camera in one sector's far field captures the near field of the next sector's camera. Additionally, vendors should ensure their PIDS uses the correct camera technologies to ensure assessment can be conducted in the near field, the assessment zone, and the far field.

[5] Alan Evans, John L. Russell & Benjamin B. Cipiti (2023) New Security Concepts for Advanced Reactors, Nuclear Science and Engineering, 197:sup1, S70-S79, DOI: 10.1080/00295639.2022.2112134

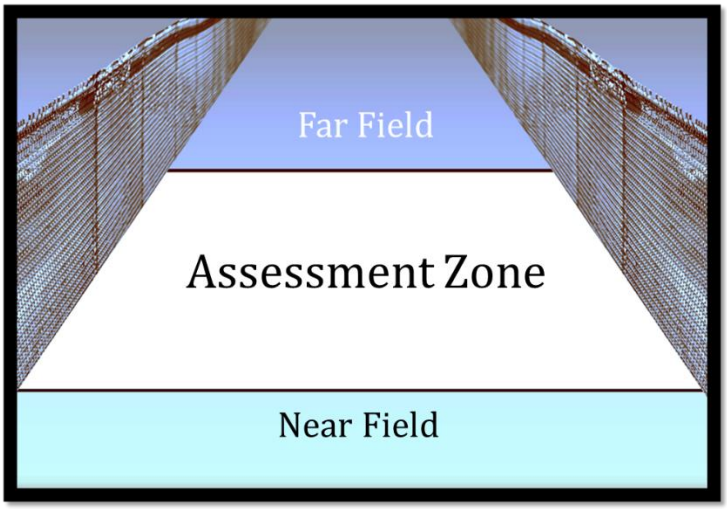

Figure 10. Monitor View of an Assessment Zone

Vendors should also ensure that their camera system allows for the classification of objects in the near field and far field of their assessment zones. Detection is the ability of the operator using the assessment system to identify that an object is present within the assessment zone. Classification is the ability of the operator to determine the type of object (e.g., person, animal). Identification is the ability of the operator to determine the identity of the object (i.e., who the person is). At the minimum, SMR and microreactor vendors should ensure that their assessment system is designed to allow for the classification of an alarm cause at the perimeter of the facility. This allows the operator to determine if the alarm is caused by a nuisance, weather event, or an actual intruder, and to begin the response to an actual security event.

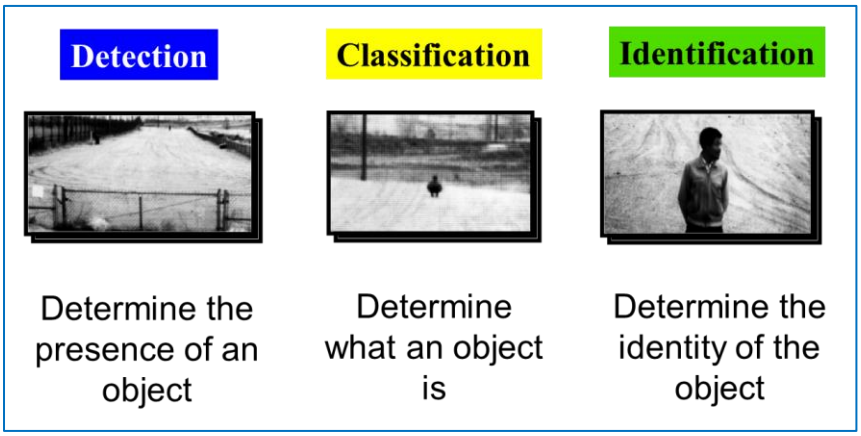

Figure 11. Levels of Resolution for Video Assessment Systems

2.5. Central Alarm Station and Backup Alarm Stations

Lesson Learned: Cost reductions may be realized through many aspects of the PPS, but SMR and microreactor vendors should consider designing a robust CAS that allows for effective assessment and communication to a response force. Additionally, SMR and microreactor vendors should consider having some form of a backup alarm station (BAS).

The CAS plays an important role for an effective PPS. The CAS should be designed in such a way that it reduces the operational burden on the CAS operator and allows the operator to effectively facilitate access control, assess the causes of alarms, and provide adequate communication to the response force. The AC&D system is the method the CAS operator uses to facilitate these functions. It is important for vendors to ensure they design the CAS with adequate room for all of the necessary equipment needed in a CAS to allow for the CAS operator to be effective. The figure below shows an AC&D setup for two alarm station operators. SMR vendors should consider the design of the CAS and the AC&D system in their overall plant design.

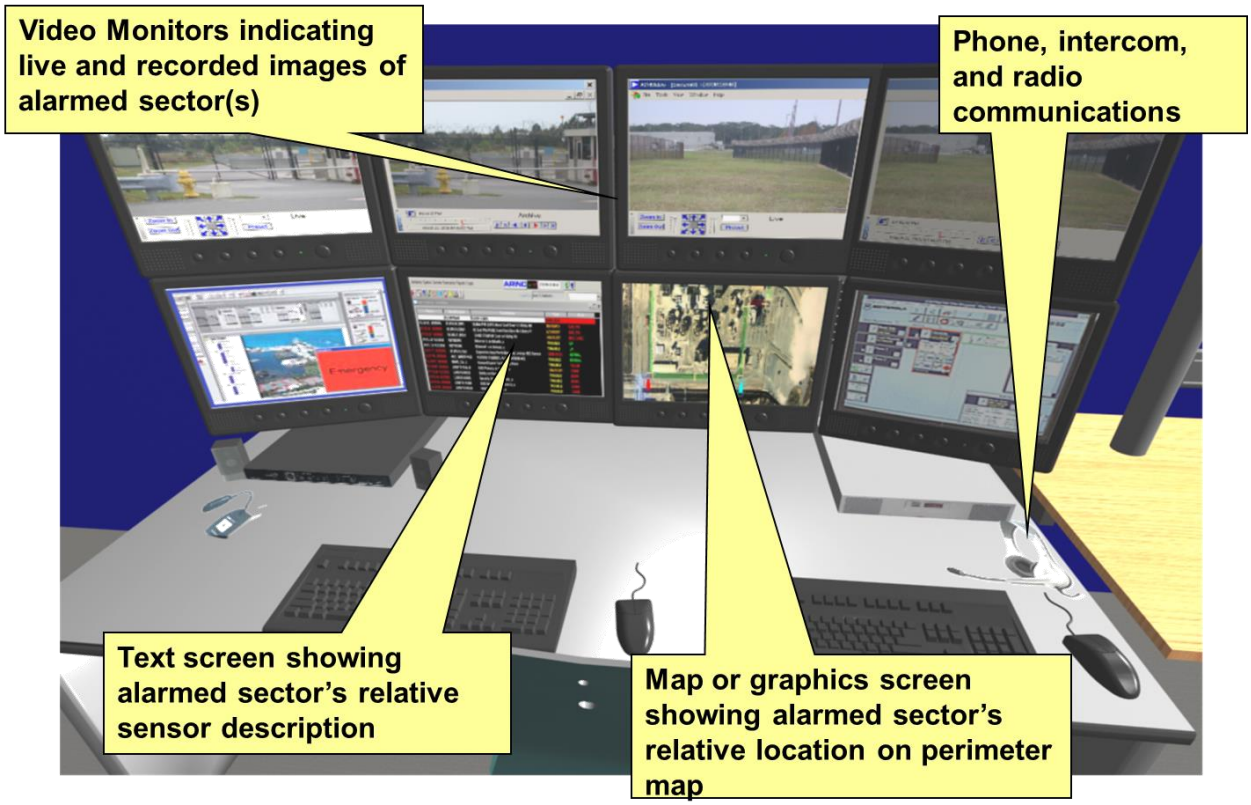

Figure 12. Alarm Communication & Display System

It is important that SMR and microreactor vendors consider designing a robust CAS that is capable of withstanding a DBT attack to ensure that the CAS operator can provide adequate and timely information to the response force. During a nuclear security event, the CAS should provide situational awareness and adversary tracking that will ensure the response force can effectively respond to the event. The CAS should be designed and placed in a location to withstand the vehicle-

borne explosive device (VBED) stated in the DBT. The CAS should also be hardened with significant delay time to decrease the probability that the adversary can take over the CAS.

It is also important for SMR and microreactor vendors to consider some form of a BAS in their design, even if not required by regulations. A BAS capability would ensure that the PPS can still operate effectively during a nuclear security event to facilitate an effective response. The BAS can facilitate alarm annunciation, alarm assessment, and response force communication if the CAS is lost. SMR and microreactor vendors should consider the events that may cause the loss of the CAS, including an adversary attack or loss of power.

3. INTEGRATED PHYSICAL PROTECTION SYSTEM DESIGN

Lesson Learned: SMR and microreactor vendors should consider integration of detection, delay, and response throughout the design of the PPS. Additionally, vendors should consider how their facility design can facilitate a more effective response force and reduce the number of responders needed to effectively interrupt and neutralize an adversary.

Many SMR and microreactor facilities are in the design phase for both their facility and PPS. A PPS is an integrated system of subsystems including detection, delay and response. A PPS must have all three functions to effectively interrupt and neutralize an adversary attack. To first create a response to a security event, the ability to detect that a malicious act is occurring is required; this includes both external and internal IDSs. The second factor is to create enough delay to allow for the response force to respond in time to interrupt an adversary force. The final factor is ensuring that the response force has adequate time to interrupt the adversary force and is then capable of neutralizing the adversary force attempting a malicious act.

During our interaction and support for SMR and microreactor vendors, it has been noticed that all vendors may not be considering the integration and interaction of detection, delay, and response when designing their PPS. Each of the PPS functions must be designed to integrate with each other to facilitate an effective PPS. For example, SMR and microreactor vendors are persistent on reducing the upfront and long-term operational costs for their PPS and may be considering designing their external IDS to not be as robust as it may need to be. A less robust IDS may allow for adversaries to bypass this line of detection and therefore reduce the number of detection points at the facility. If the number of detection points at the facility is decreased, the critical detection point (CDP) may be missed and not allow for a timely response to a security event at the facility. The CDP is the last sensing opportunity in the PPS that allows for assessment, communication, and for the response force to arrive in time to interrupt the adversary. The CDP may need to move closer to the target location and require the design of additional delay barriers, or it may require the vendor to consider the use of an onsite response force to effectively interrupt and neutralize the adversary force. The figure below shows an example of an adversary task time compared to the PPS response time. As can be seen, as the first sensing opportunity is placed later in the adversary task time, the result is response time may not be adequate to respond to a security event.

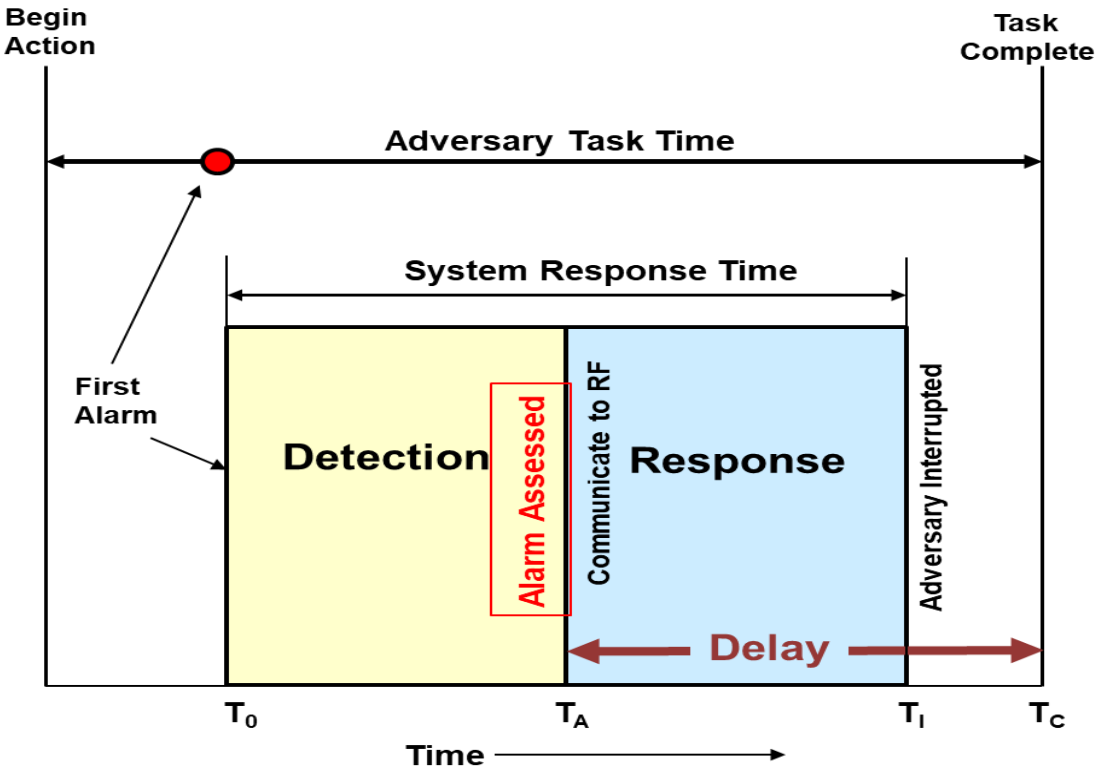

Figure 13. Adversary Task Time Compared to PPS Response Time

Another point of integration to be considered is the vehicle barrier system, including the design of the perimeter and its impact on the response force at the site. If an SMR or microreactor vendor is designing their PPS strategy based on using an onsite response force, the designers should evaluate how the perimeter design of the facility will impact the ability of the onsite response force to respond to a security event. For example, SMR and microreactor vendors may want to decrease the size of their facility perimeter and protected area to decrease costs. This reduction in perimeter size may decrease the open space that an adversary may have to cross and therefore decrease the effectiveness of the response force. Through vendor engagements and studies conducted in the ARSS program, we have learned that increasing the open space around the facility and minimizing locations where the adversary can find cover/concealment can improve the probability that the response force is able to neutralize the adversary force. Creating open-space areas that the adversary must cross will increase the likelihood the response force can neutralize the adversary and decrease the probability that an adversary is able to neutralize a responder engaging from a position of cover. Additionally, vendors should consider limiting the obstructions for onsite responders in fixed positions to view the protected area perimeter. This would allow for the responders to have clean field-of-view to engage an adversary force and the ability to potentially act as a compensatory measure to view the perimeter of the facility in the event the PIDAS is lost.

3.1. Building Design and Response Force Strategy

Lesson Learned: Designing single building sites in a square or rectangle configuration can help improve PPS effectiveness and may lead to reduced overall staffing headcounts at an SMR or microreactor facility.

SMR and microreactor vendors are interested in reducing the overall staffing headcount to reduce the costs to operate and SMR or microreactor. This may include reducing the headcount of the response force and armed security officers (ASOs). These positions can become costly, as considerations must be made for 24/7 availability. Traditionally, each 24/7 position required in the security plan considers a full-time equivalent (FTE) multiplier of 4–4.7. In the example below, if four armed responders are required by the security plan, then the facility may have to have 16–19 responders paid full-time to provide response to the facility. During our vendor engagements and general research to develop cost-effective PPSs, one method to help realize headcount reductions is reducing the footprint of the facility as much as possible and utilizing a single building that is square or rectangular in shape. Figure 14 shows a hypothetical SMR design utilizing a square building design with four responders in the corners of the building structure.

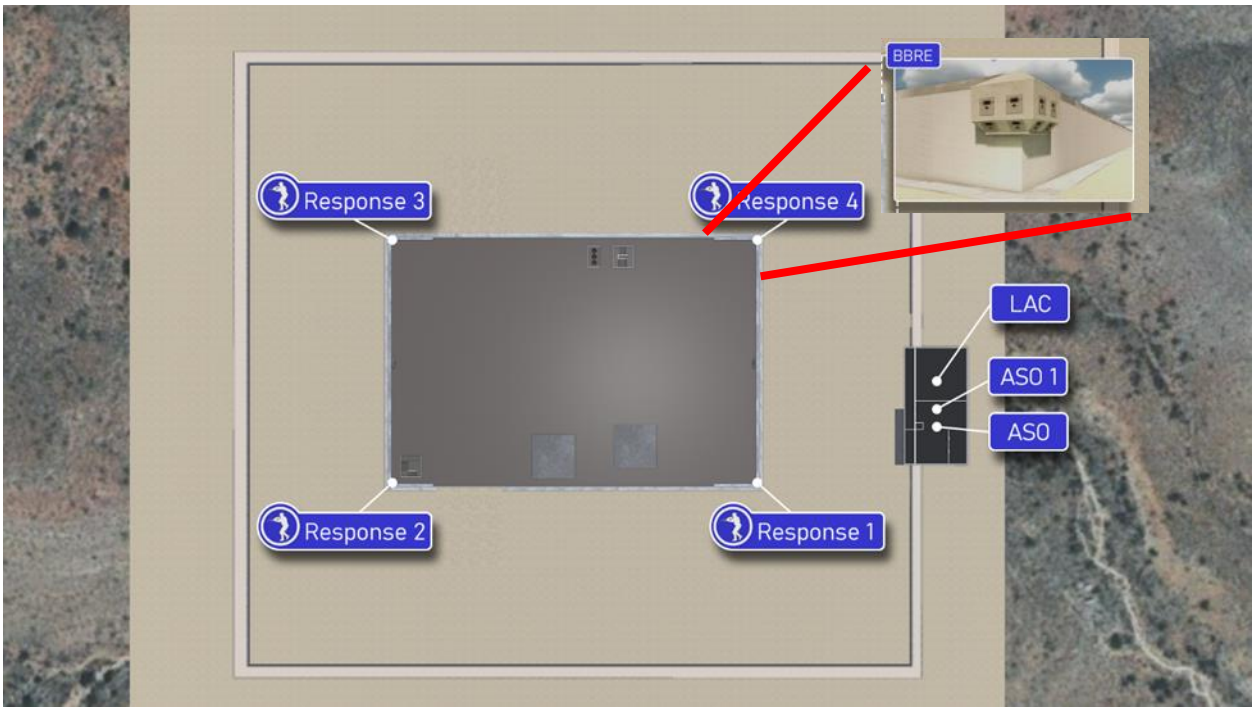

Figure 14. Square Building Design

From this figure, it can be seen that the facility has no obstructions blocking the line-of-sight for the responders to the perimeter, and the responders are located in bullet- and blast-resistant enclosures (BBREs). These BBREs provide the responders cover and additionally have a similar structure on the inside of the facility. Because of the covered position for the responders and lack of obstruction from the BBREs to the perimeter, the responders are able to have line-of-sight to the perimeter acting as a compensatory measure, and the adversary must cross a large open-space area with no cover up to the outside of the building. This provides the response force with ample time to engage an adversary force and may increase the probability the response force can neutralize an adversary force. Additionally, utilizing a rectangular or square building design minimizes the number of credible pathways the adversary can take to gain entry into the building and therefore allows for the PPS design and response force strategy to be more effective, leading to a reduced number of required security personnel.

3.2. Staffing Plans

Lesson Learned: A commercial nuclear power plant (NPP), regardless of physical site size or electrical output, will require substantial onsite security staff to fulfill the performance requirements outlined in the regulations. However, through mindful design choices, staffing can be optimized while accounting for contingencies to satisfy the security plan.

When designing a PPS, it can be easy to solely focus on the number of committed responders as a basis to calculate headcount. Below is the current minimum headcount required by 10 CFR 73.55:

- Security Shift Supervisor
- Response Team Leader
- Central Alarm Station Operator
- Secondary Alarm Station Operator
- 10 Armed Responders
- Last Access Control (may be one of the 10 armed responders)

A typical staffing multiplier used is 4 headcount per position on 12-hour shifts, which includes training, turnover, and benefit time. This results in a headcount of 63 to meet the minimum regulatory standards. If the current regulation is revised or an exception is granted, the number of responders is likely the only number that can be reduced. These minimum staffing numbers are outlined in Table 1.

Table 1. Required NRC Security Positions under 10 CFR 73.55

Position	24/7 12-hr rotating shift	Total FTEs
Security Shift Manager	1	4
Field Supervisor/Response Team Lead	1	4
Alarm Station Operators	2	8
Armed Responders	10	40
Armed Security Officers (Personnel, vehicle, and material processing)	2	8
Total	**16**	**64**

This table identifies the minimum for protecting the plant and does not include those needed to support daily plant operations. The following is a list of considerations for staffing at an operational NPP. A few of the considerations are detailed below.

1. Total system failure
2. Personnel access
3. Vehicle and material access and escort

3.2.1. Total System Failure

Total system failure is the loss of all detection and assessment capabilities. Compensatory measures equal to or greater than those provided by the system must be established within a short timeline. Some U.S. NPPs use this as their basis for minimum staffing. The response to a total system failure can consist of posting all protected area perimeter segments with armed personnel in protected positions. This is often why elevated, hardened defensive positions are selected for exterior defense. If all segments can be observed from these positions, then no additional personnel are needed for the perimeter. In addition, interior patrols for vital area barriers and portals may be necessary and, based on operational needs, some vital area access points may need to be posted. Compensatory responsibilities for a total system failure may be included within the contingency plan as part of the overall site security plan.

3.2.2. Personnel Access

The personnel access point must be staffed when personnel need to access the protected area, which for large sites may be continuously. Security personnel must observe the search process, respond to metal and explosive detector alarms, and perform hand searches when required. This can be operated by one person with dedicated overwatch from the Last Access Control position, but the search process would be very slow. This may be acceptable on weekends and back shifts or for sites with extremely low numbers of operational personnel. However, for sites with a large operational footprint (including maintenance, operations, radiation protection), this could require a significant number of personnel. None of these security persons can be included in the minimum number of responders because they are outside of the protected area. Furthermore, there may be issues with assigning them access control duties when this could be perceived to interfere with their duties as responders.

3.2.3. Vehicle and Material Access and Escort

Vehicle and material access points are only staffed when needed but require a minimum of two security persons (search and overwatch), which are not counted in the minimum number of responders. These are typically staffed during high traffic times (e.g., Monday–Friday day shift). This does not include the potential need for vehicle and material escorts. Vehicle escort may be performed by the search overwatch person or the search person and must be armed. While the vehicle and material access points are not required to be staffed at all times, personnel should be available to post these positions 24/7 to provide emergency vehicle ingress and egress in the event of a plant or medical emergency. This should be described in the site's Emergency Response Plan.

To account for potential unexpected unavailability of responders or other security personnel, it would be prudent for a licensee to include on-call or surplus onsite staffing to be able to satisfy the regulations and the security plan in case of any contingencies. Table 2 shows a security staffing headcount that meets the requirements in 10 CFR 73.55 and includes additional security personnel per shift to provide defense-in-depth to effectively operate the PPS.

Table 2. Accounting for Anomalies Meeting NRC Regulations in 10 CFR 73.55

Position	24/7 12-hr rotating shift	Total FTEs
Security Shift Manager	1	4
Field Supervisor/RTL	2	8

Position	24/7 12-hr rotating shift	Total FTEs
Alarm Station Operators	3	12
Armed Responders	12	48
Armed Security Officers (Personnel, vehicle, and material processing)	4	16
Total	22	88

Table 2 shows that a large amount of security staff is necessary to realistically operate a PPS at an SMR facility. However, SMRs may have the ability to reduce the total number of personnel required to implement an effective PPS through exemptions to certain regulatory requirements while still being able to adequately satisfy the intended overall performance requirements. SMRs, due to their smaller nature, reduced number of targets, and reliance on safety systems may be able to reduce the total number of security personnel (mostly armed responder reductions). Table 3 shows an alternative security staffing headcount for a hypothetical SMR with exemptions from the existing regulatory requirements in 10 CFR 73.55.[6]

Table 3. Alternative Security Staffing Headcount

Position	24/7 12-hr rotating shift	Total FTEs
Security Shift Manager	1	4
Field Supervisor/RTL	2	8
Alarm Station Operators	3	12
Armed Responders	6	24
Armed Security Officers (ECP, Vehicle Search, Escorts)	3	12
Total	16	60

[6] "U.S. Domestic Sodium Fast Reactor: Security-by-Design." Evans A., Horowitz, S. Stromberg B., Steagall I., Abell D., Davenport J., Sweet S. Sandia National Laboratories, SAND2023-09146R

4. CONCLUSIONS

SMR and microreactor vendors face unique deployment challenges that will impact the security system design. In our engagements with SMR and microreactor vendors, we have noted many lessons learned that can provide recommendations to all SMR and microreactor vendors.

SMR and microreactor vendors should consider the deployment location of their reactors and how the deployment location will impact the design and operation of the PPS. The deployment location could impact the security technologies that are chosen, the ability to trench power and communication cables, and what type of response force strategy can be effective. The deployment location may also impact the ability of the adversary to delay the response force, or if remote enough, could offer a measure of deterrence to attacking this type of facility.

SMR and microreactor vendors should consider designing a robust PIDS that is capable of detecting adversaries, communicating a nuclear security event to the response force, and provide situational awareness to the response force during a nuclear security event. SMR vendors should evaluate choices of sensors, cameras and AC&D systems to ensure that these capabilities exist and can aid in increasing the effectiveness of the PPS. Additionally, SMR and microreactor vendors should design their CAS to be capable of surviving the DBT VBED and be provided with enough delay time to ensure that adversaries cannot sabotage or compromise the CAS. SMR and microreactor vendors should also consider having a BAS, regardless of regulatory requirements, to ensure there is a contingency measure to receiving alarm communications and assess alarms in the event the CAS is lost.

SMR and microreactor vendors should also consider the integration of all subsystems of the PPS into their overall design. Many SMR and microreactor vendors are interested in the reduction of up-front and long-term security costs but may not be considering how the systems being designed can complement each other and provide cost reductions. The integration of the PPS design should not only be integrated with each subsystem, but also with the operations and safety design of the facility as well. Modifications to the plant layout can have drastic effects on the PPS design and may reduce operational costs but may lead to an increase in up-front and long-term security costs.

Email—Internal

Name	Org.	Sandia Email Address
Alan Evans	06812	aevans@sandia.gov
Technical Library	01977	sanddocs@sandia.gov

This page left intentionally blank.


Sandia
National
Laboratories